UNITED STATES DEPARTMENT OF AGRICULTURE

Personal Electronic Device (PED) Security Assessment Guide

September 6, 2001

Prepared by:
Barre Bull, Tech. Director for InfoSec Svcs.
Chuck Cramer, IT Security Analyst

Science Applications International Corporation
An Employee-Owned Company
13921 Parkcenter Rd., Suite 300
Herndon, VA, 20171

SAIC-6663-2001-122

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

For Official Use Only

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Personal Electronic Device (PED) Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, “USDA Information Systems Security Policy.” By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Personal Electronic Devices (Portable Laptop Computers, Personal Digital Assistants (Palm Top and Handheld), and Cellular Telephones) connecting to USDA LAN resources. The checklist addresses both USDA issued and personal owned systems. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if devices meet the requirements for connectivity to a Sensitive But Unclassified (SBU) systems and assessing the vulnerabilities, both current and potential, they bring to the systems. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data and systems.

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources.” A security risk assessment process is a comprehensive evaluation of the system’s technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements.

4. REFERENCES

a. External

(1) Public Law 100-235, “Computer Security Act of 1987.”
(2) Public Law 93-579, “Privacy Act of 1974.”
(3) Public Law 93-502, “Freedom of Information Act.”
(4) Public Law 99-474, “Computer Fraud and Abuse Act.”
(5) OMB Circular No. A-130 Appendix III, “Security of Federal Automated Information Resources,” revised February 8, 1996.
(6) OMB Circular No. A-123, “Management Accountability and Control,” June 29, 1995.

(7) FIPS No. 140-1 “Security Requirements for Cryptographic Modules,” January 11, 1994.

b. USDA Internal Regulations

(1) DR 3140-001, “USDA Information Systems Security Policy” dated May 15, 1996.
(2) DR 3300- 1, Appendix I, “USDA Telecommunications and Internet Services and Use,” March 23, 1999.
(3) DM 3140-1 “USDA Management ADP Security Manual” dated March 5, 1992.
(4) DN 3120-1 “USDA Technical Standards Architecture,” dated April 3, 1998.

Personal Electronic Device (PEDS) Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency/System Identification:

Agency (Agency, Office, Bureau, Service, etc.):	
Address	
Date of last Assessment:	

Test Number: **1**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Basic Policy Procedures for Personal Electronic Devices (PED)			
Resources Required:	Local policies for PED systems.		
Personnel Required:	Systems Administrator/Information Security Personnel		
Objectives:	To determine if general policies and procedures are established to control the use of PED systems in the USDA.		
Procedure Description: (Summary)	Verify that policy is in place addressing the use of USDA owned and privately owned PED systems, and to verify that appropriate security measures are taken when connecting PED systems to USDA resources.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Are policies established authorizing personnel to use PED systems?	Written policy establishes policy for personnel to use PED systems to accomplish work related tasks.		
2.	Are policies established to authorize connectivity between PED systems and USDA ADP resources (Remote and direct connect)?	Written policy authorizes personnel to access USDA ADP resources using PED systems.		
3.	Are policies established for requesting access to USDA ADP resources using PED systems?	Written policy addresses procedures for requesting access to USDA ADP resources using PED systems. Procedures should include a systematic process of requesting		
4.	Do policies address functionality and performance standards for PED systems?	Written policy addresses minimum and authorized functionality and performance standards for PED systems (I.E. CPU speed, RAM requirements, storage space, modem requirements, operating system requirements).		
5.	Are adequate PED security standards for both systems administrators maintaining Remote Access Services (RAS) and individual users addressed in USDA policy?	Written policy address adequate security standards used by both systems administrators and users of PED systems.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
6.	Do policies address use of privately owned PED systems to access USDA ADP resources?	Written policy authorizes personnel to use privately owned PED systems to access USDA ADP resources.		
7.	Are training standards established for PED usage and security?	Written training plans address PED usage and security procedures. At a minimum, training programs should address basic security fundamentals, physical security, access procedures, request for use procedures, and course of action plans for lost or stolen PED systems.		
8.	Are written policies established for the accountability, disposal, maintenance, and safeguarding of PED systems?	Written policy addresses procedures for accounting for, disposing of, and maintaining of PED systems.		
9.	Do written policies authorize PED system access to USDA ADP resources through outside internet service providers?	Written policy addresses the use of privately acquired service providers to access USDA ADP resources.		
10.	Do written policies address procedures for personnel to access RAS with PED systems?	Written policy addresses step-by-step procedures for personnel to access USDA ADP resources using remote access.		
11.	Are procedures outlined in the ADP incident response plan for lost or stolen PED systems?	Incident response plans should include immediate steps to take in the event of a reported lost or stolen PED system. At a minimum, the plan of action should include immediate closure of the users account, accessing the amount of information lost with the system, and procedures for obtaining a user incident report.		
12.	Have legal concerns regarding search and seizure of privately owned PED systems been addressed	A legal opinion regarding the search and seizure of privately owned PED systems is available.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	through legal services?			
13.	Are policies and procedures pertaining to PED systems current?	Policies and procedures are up-to-date.		
14.	Are frequent audits and vulnerability tests conducted to determine the efficiency and effectiveness of wireless and RAS security plans?	Frequent audits and vulnerability tests are conducted to ensure that policies are adhered to. In particular, the following areas should be frequently reviewed: user access, access point vulnerabilities, and equipment functionality.		

Comments:

Action Plan:

Test Number: **2**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Remote Access Services (RAS) (Dial-in, VPN, Wireless, Infrared (IrDA)			
Resources Required:	Established remote access.		
Personnel Required:	Network Administrator		
Objectives:	To determine if remote access points are properly configured. To determine if remote access points meet required security standards.		
Procedure Description: (Summary)	Verify remote access point policies and configurations to ensure efficient and secure access by remote users.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Are dedicated resources selected to support the RAS (access points, servers, firewalls, modems, and routers)?	Dedicated resources should be identified for RAS access. Dedicated equipment will help to reduce security risks to systems used by internal users.		
2.	Are adequate security and architecture standards for the RAS published in the written computer support plan?	Adequate security standards are published in local policy and reflect requirements for end-to-end security.		
3.	Are Systems Administrators knowledgeable of wireless technology?	Systems administrators should have an understanding of wireless functionality to include, but not limited to, Wireless Access Protocol, Wireless Equivalent Privacy, Wireless Markup Language, IEEE 802.xx standards, and “Bluetooth” security.		
4.	Is the RAS designed to provide end-to-end security for wireless communication?	Wireless security sets should be configured for end-to-end security including encryption and decryption		
5.	Do systems supporting the	Computers meet local		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	RAS meet established functionality and performance standards?	functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
6.	Do computer architecture plans for RAS support include segmenting equipment in a secure architecture format such as "DMZ"?	Segmenting equipment dedicated to providing RAS support. Dedicating resources to specific functions in support of the RAS decreases the potential for external attacks on local internal resources.		
7.	Are server systems tasked with handling RAS properly configured for only selected services? SMTP Access Points FTP HTTP HTTPS TELNET	Operating systems are configured per local and manufacturers specifications to provide optimum and secure performance. Systems administrators make frequent checks to ensure that operating systems are up-to-date with new security/ software patches.		
8.	Are appropriate server operating systems selected to support VPN and remote dial-in services?	Software and operating system packages should be selected that will provide optimum service for both client and server.		
9.	Are server software applications properly configured to manage RAS?	Servers and software applications are configured to allow only those services designated for remote access.		
10.	Are firewall security systems properly configured for the RAS?	Remote access servers are protected by firewall security. The firewall is configured to allow only authorized traffic through.		
11.	Are router policies properly configured to provide secure wireless and VPN support?	Routing systems are configured according to local and manufacturers specifications to		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		support remote access. Decisions as to the extent of security provided by router support will dictate the required settings. Routers can be configured to allow pass-by of remote authentication procedures or can be configured to handle a portion of the process (Not Recommended)		
12.	Are configuration rules periodically checked for all systems to ensure they continue to meet local policy, manufacturers specifications, and upgraded changes to support security concerns?	Software applications, servers, firewalls, and routers supporting the VPN should be all checked periodically for upgrades and patches.		
13.	Do systems supporting the RAS have updated virus scan software with updated signatures?	“Strong virus” protection software with updated signatures is installed. Administrators should pay particular attention to procedures for scanning uploaded files from remote clients.		
14.	Are procedures outlined in the incident response plans in the event of systems failures for equipment supporting the RAS?	Course of action plans are in place to handle disruption of services.		
15.	Do RAS authentication protocols meet local security needs?	Authentication protocols should meet local policy requirements. Recommended use of a RADIUS type authentication protocol for wireless.		
16.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users and systems administrators are required to frequently change their passwords (min 30 days), and follow specific design guidelines per local		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		regulation.		
17.	Are encryption devices and keys changed out frequently?	At a minimum, encryption keys should be changed every two weeks. Dynamically created keys are preferred over static keys as they can be changed on a per session basis. Where physical devices such as smart cards are used, best practice recommends bi-weekly to monthly changes.		
18.	Do personnel accessing USDA resources through the RAS authorized in writing?	Request forms should contain at a minimum supervisor, systems administrators, and users signatures.		
19.	Does the system administrator maintain a log of personnel authorized to access the RAS?	Systems administrators maintain a copy of the user request form.		
20.	Are frequent checks made of remote access account logs to ensure that unused or expired accounts are removed?	Expired accounts are removed, and a system is established to ensure that users who have departed the USDA are removed from the RAS access list.		
21.	Are personnel allowed access to only those resources required to meet job requirements?	Personnel are restricted to only those resources required to meet task requirements.		
22.	Are personnel restricted from making multiple “same time” connections to the RAS?	Users should not be allowed multiple login capabilities. An exception would be systems administrators who normally use multiple logins for troubleshooting.		
23.	Are dial-in and VPN access times established?	Where resources and support personnel are limited, access times should be established.		
24.	Has a dial-up protocol been selected that will efficiently and effectively support local dial-in requirements?	A dial-in protocol should be selected that will meet dial-in and security requirements.		
25.	Are modem pools established and configured properly to support dial-in access.	Modem pools are established for remote dial-in service based		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		upon demand.		
26.	Are modem access numbers maintained in a secure area, and are numbers unlisted?	Modem access numbers should be kept in a secure location and periodically changed where possible.		
27.	Do systems administrators maintain audit logs for system performance, intrusion detection, and succeeded and failed login attempts, and user access times?	Systems logs are available for review.		
28.	Are external vulnerability scans conducted to determine weak points?	Vulnerability scans are conducted on a regular schedule basis and at a minimum, when systems changes are made.		
29.	Are intrusion detection strategies implemented for the RAS?	Intrusion detection procedures for remote services are included in the organizational intrusion detection and response plan.		
30.	Are VPN's used in conjunction with Wired Equivalent Privacy procedures to provide additional security?	VPN's are a sound means for creating encrypted and secure transfer of data from local resources to remote clients.		
31.	Are VPN's configured per manufacturer's and local policy standards to obtain optimum security and efficiency for wireless access?	The VPN architecture and configuration should be per local policy and manufacturer recommendations. A poorly configured VPN can leave local resources extremely vulnerable to outside security breaches.		
32.	Are site VPN's used to allow access to local resources by remote field offices?	If properly configured, a site supporting VPN can be an effective and efficient means to provide outside access by trusted agencies or remote USDA field offices.		
33.	Do policies address the development of site VPN's?	Site VPN's require the same if not greater security measures as		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		private connected VPN services. Policies should address restrictions similar to those required of remote single client users.		
34.	Have VPN protocols been selected based upon the type and level of security required (IPsec, PPTP, L2TP, etc.)?	Protocols have been selected based upon needs.		
35.	Are strict restrictions placed on what resources are available to site VPN's?	As with individual client connections, restrictions should be placed on what areas are offered to site VPN users.		
36.	Does the server/firewall architecture supporting the additional encryption/ decryption for inbound site VPN traffic meet standards to manage additional loads?	The encryption/ decryption process for authenticating and transferring data to and from site VPN's is a demanding process that can diminish the effectiveness of systems being used to support local resources.		
37.	Are coherent addressing schemes developed for both remote and local VPN sites?	Addressing schemes are configured to avoid collision of IP addresses during transfer of data.		
38.	Are VPN's providing site service monitored to ensure that they are operating smoothly?	Systems are monitored to ensure that they are functioning properly per local and manufacturers specifications. Substandard functioning VPN's can create additional drain and flaws in local architecture plans.		

Comments:

Action Plan:

Test Number: **3**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Laptop Systems			
Resources Required:	Access to laptop computer systems.		
Personnel Required:	Systems Administrator/Laptop User		
Objectives:	To determine if laptop computers meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of laptop computers in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Do laptop computers meet established functionality and performance standards?	Laptop computers meet local functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused laptop systems stored in a secure location?	Laptop computers are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists available showing complete serialized listings of all peripherals and internal components for all laptop systems.		
4.	Are published laptop checkout procedures followed?	Users have completed the required request form for acquiring laptop systems.		
5.	Are laptop systems “scrubbed” of previous user data prior to turn-in?	Prior to turn-in or checkout, laptop systems should be checked to ensure that user profiles, user data files, and “user unique” software applications are removed.		
6.	Are system/application security features pre-configured for the user?	Applications used to access local resources are properly configured.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
7.	Are systems with dial-in/wireless modems pre-configured using the proper configurations?	Modem software is properly configured.		
8.	Are policies established granting users authorization to add peripherals and software?	Policies are in place defining what peripherals and software users can add to laptop systems.		
9.	Are users restricted from making certain system configuration changes?	Policies have been established restricting users to making only configuration changes necessary to accomplish assigned tasks.		
10.	Are data/file synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
11.	Do users receive training on laptop usage and security requirements?	Verification that the user has been trained in basic functionality and data security requirements.		
12.	Do users understand the RAS requirements and procedures?	The user understands all procedures for the “type” of remote access in use. Identified in a signed statement or training attendance form.		
13.	Do users understand authentication procedures to access local resources?	The user understands the proper authentication procedures for accessing local resources through the RAS.		
14.	Is the user required to enter a password to enter the system BIOS area?	Laptop BIOS areas are password protected.		
15.	Is the user required to enter a password to enter the system boot process?	Prior to boot-up, the user must enter a password. Where applicable, some systems include the added feature of securing the hard drive with a password. If available, this feature should also be activated.		
16.	Is the user required to enter a	Prior to entering the		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	password prior to accessing the operating system/LAN?	operating system and logging into LAN resources, the user is required to enter a password.		
17.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
18.	Does a locally established "Warning Statement" appear during the boot process?	Laptop systems contain a local established "Warning Statement." Example located at Appendix 1.		
19.	Are individual firewall software applications installed?	For added protection, adding a personal firewall program such as "Black Ice Defender", "Zone Alarm", or "Norton Personal Firewall" will add additional protection.		
20.	Are multiple user accounts properly configured on shared systems?	Laptops checked out for use by multiple personnel should have individual profiles created. Profiles should be configured for individual needs and access rights.		
21.	Are only authorized software applications installed?	Only authorized software applications are installed.		
22.	Are encryption/decryption procedures used when data is stored on the laptop?	Confidential information is stored in an encrypted state.		
23.	Are at least 128-bit algorithms used for data encryption/decryption?	Systems should be equipped with 128-bit encryption capabilities for data encryption.		
24.	Are data files encrypted on a per record basis?	Systems should decrypt only those records being used. If the system were stolen or lost, a would-be thief will have limited access to only the current working document.		
25.	Are users restricted from	Users should not be		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	disabling encryption settings on a per-application basis?	allowed to change encryption settings.		
26.	Are system files/directories tagged as “read only”?	System files are marked as read only.		
27.	Are only authorized and up-to-date software applications installed?	Laptop systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
28.	Is the required virus protection software installed with an updated signature file?	Laptop systems have the required virus protection software with an updated signature file.		
29.	Is the system screensaver/ password combination process activated?	System screensaver/password function is enabled.		
30.	Are authentication procedures established for linking to USDA ADP resources through laptop systems?	Mutual authentication is required prior to obtaining access. This requires a clear acknowledgement of both the RAS system and the client system before access is granted.		
31.	Is the user authorized in writing to access USDA resources through the RAS?	Written authorization allowing the user to access USDA resources is required.		
32.	Are users accessing the RAS authorized access into only certain resources?	Remote access should be limited to only those file areas required to accomplish job related tasks.		
33.	Are there established access hours for remote users?	RAS servers are configured to allow access during only authorized times.		
34.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
35.	Are systems properly disposed of per local policy?	Laptop systems found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
36.	Are users instructed on procedures to take in cases of lost or stolen laptop system?	Users understand the course of action for reporting lost or stolen systems per local policy.		
37.	Are procedures established for allowing personnel to connect internally (from their own office space) to USDA ADP resources using laptop systems?	Written authorization allowing the user to access resources.		
38.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned laptop systems to receive prior approval?	Personnel requesting to use privately owned laptop systems to connect to resources require the same prior approval as those personnel using organizational issued laptops.		
39.	Are privately owned systems required to meet the same functionality/performance standards as organizational issued laptops?	Policy addressing requirements for personally owned laptop systems listing the minimum acceptable standards.		
40.	Are privately owned laptops systems checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned laptops systems are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required configuration settings to connect through local resources or external dial-in/VPN.		
41.	Are owners of privately owned laptop systems informed that their systems are subject to periodic security checks?	Personnel using privately owned laptops should be under the same guidelines as organizational issued laptops with regards to periodic security checks to ensure that conformance standards are being met.		
42.	Are the same security requirements established for organizational issued laptops required for privately owned systems?	Users of privately owned laptop systems should have the same security requirements to connect to local		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:
Action Plan:

Test Number: **4**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Wireless Phones with Internet Capability			
Resources Required:	Cellular phone with access rights to local resources.		
Personnel Required:	System Administrator and Cellular Phone User with Internet connection capabilities.		
Objectives:	To determine if cellular phone systems meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of cellular phone systems in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Is there an established functionality and performance standard for cellular phone systems?	Cellular phones used for internet/intranet connectivity to USDA resources meet written functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused cellular phones stored in a secure location?	Unused cellular phones are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists are available showing complete serialized listings of all peripherals and internal components for all cellular phones.		
4.	Are published cellular phone checkout procedures followed?	Users have completed the required request form for acquiring cellular phones.		
5.	Are systems “scrubbed” of previous user data prior to turn-in?	Cellular phones with storage capabilities should be scrubbed of all data prior to turn-in. Prior to placing a system back into		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		circulation for reissue, all records/data from previous users should be discarded.		
6.	Is there an operating system password requirement for login?	Prior to entering the operating system and logging into LAN resources, the user is required to enter a password.		
7.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
8.	Are mutual authentication procedures established for linking in with USDA resources through cellular systems?	Mutual authentication is required to obtaining approval to access.		
9.	Are 128-bit Advanced Encryption Standard algorithms used for data encryption?	Systems should be equipped with 128-bit encryption capabilities for data encryption.		
10.	Are only authorized and up-to-date software applications installed?	Cellular systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
11.	Is the required virus protection software installed with an up-to-date signature?	Cellular phones have the required virus protection software with updated signature files.		
12.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
13.	Are policies established restricting users from making certain configuration changes?	Users are authorized to make only minor adjustments to systems, and only those adjustments necessary to accomplish assigned tasks.		
14.	Are policies established granting users authorization to add peripherals and software?	Restrictions are in place showing what peripherals and software users can add		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		to cellular phones.		
15.	Do users receive training on cellular phone usage and security requirements?	Verification that the user has been trained in basic functionality and data security requirements.		
16.	Are security standards established for cellular phone connectivity to USDA ADP resources?	End-to-end and adequate security measures are established for connectivity to local resources.		
17.	Are cellular phone connections to USDA ADP resources authorized through private domain services (Individual VPN services)?	Access to resources is authorized through private domain services following strict guidelines to accomplish organizational tasks.		
18.	Are data synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
19.	Are user profiles properly configured for docked/un-docked status?	User profiles are configured according to manufacturers and local policy specifications.		
20.	Are there established access hours for cellular phones to connect through to the RAS?	Remote access servers are configured to allow access during only authorized times.		
21.	Are system/application security features pre-configured for the user by an experienced technician?	Software and hardware are both pre-configured		
22.	Are users restricted from disabling encryption settings on a per-application basis?	Users should not be allowed to change encryption settings.		
23.	Do systems provide per record decryption capabilities?	Systems should decrypt only those records being used. If the system were stolen or lost, access would be limited to only the most recent working record.		
24.	Are systems properly disposed of per local policy?	Cellular phones found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
25.	Are records available showing	Systems technicians		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	prior system security/ functionality checks?	have updated reports of systems maintenance/ security/functionality checks.		
26.	Are organizational cellular phone logs checked for authorized activity?	Logs are checked for unauthorized or suspicious usage.		
27.	Are users instructed on procedures to take in cases of lost or stolen cellular phone?	Users understand the course of action for reporting lost or stolen systems per local policy.		
28.	Are systems properly disposed of per local policy?	Cellular phones found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
29.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned cellular phones to receive prior approval?	Personnel requesting to use privately owned cellular phone systems to connect to local resources require the same prior approval as those personnel using organizational issued cellular phones to connect to resources.		
30.	Are privately owned cellular phone systems required to meet the same functionality/ performance standards as organizational issued cellular phones?	Policy addressing requirements for personally owned cellular phone systems listing the minimum acceptable standards.		
31.	Are privately owned cellular phone checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned cellular phone are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required configuration settings to connect through local resources or external dial-in/VPN.		
32.	Are owners of privately owned cellular phone systems informed that their systems are subject to periodic security checks?	Personnel using privately owned cellular phones to access local resources should be under the same guidelines as		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		organizational issued cellular phones with regards to periodic security checks to ensure that conformance standards are being met.		
33.	Are the same security requirements established for organizational issued cellular phones required for privately owned systems?	Users of privately owned cellular phone systems should have the same security requirements to connect to local resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:

Action Plan:

Test Number: **5**	SITE/SYSTEM:	DATE:	TIME:
Test Name: Personal Digital Assistant (PDA)			
Resources Required:	A PDA with authorized access rights to local resources.		
Personnel Required:	Systems Administrator/Authorized PDA user.		
Objectives:	To determine if PDA systems meet USDA requirements for use and connectivity with local area resources.		
Procedure Description: (Summary)	Verify that procedures are in place for the secure use of PDA systems in both a remote and local area setting.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Is there an established functionality and performance standard PDA systems?	PDA's used for internet/intranet connectivity to USDA resources meet written functionality and performance standards. This would include items such as minimum CPU operating speed, minimum RAM memory, authorized operating systems, and authorized peripherals.		
2.	Are unused PDA systems stored in a secure location?	Unused PDA systems are stored in a secure location.		
3.	Are strict accountability procedures in place with serialized lists for systems and their peripherals?	Itemized lists are available showing complete serialized listings of all peripherals and internal components for all PDA systems.		
4.	Are published PDA checkout procedures followed?	Users have completed the required request form for acquiring a PDA system.		
5.	Are systems "scrubbed" of previous user data prior to turn-in?	Prior to turn-in or checkout, PDA systems should be checked to ensure that user profiles, user data files, and "user unique" software applications		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		are removed.		
6.	Is there an operating system password requirement for login?	Prior to entering the operating system and logging into LAN resources, the user is required to enter a password.		
7.	Are passwords established according to local policy as to size, content, and period of availability?	Passwords conform to local policy and procedure. Users are required to conform to established policy and change passwords per local regulation.		
8.	Are individual firewall software applications installed?	For added protection, adding a personal firewall program such as “Black Ice Defender”, “Zone Alarm”, or “Norton Personal Firewall” will add additional protection.		
9.	Are mutual authentication procedures using at least 128-bit encryption standards established for connecting with the RAS?	Mutual authentication using 128-bit encryption is the standard requirement.		
10.	Are 128-bit Advanced Encryption Standard algorithms used for data encryption?	Systems should be equipped with 128-bit encryption capabilities for data encryption.		
11.	Is confidential information immediately removed from the system clipboard or memo pad?	Systems should not maintain any confidential information in the clipboard or memo pad.		
12.	Are only authorized and up-to-date software applications installed?	PDA systems contain only software applications approved by local policy. Frequent checks are made for patches and updates.		
13.	Is the required virus protection software installed with an up-to-date signature?	PDA systems have the required virus protection software with updated signature files.		
14.	Are system maintenance/ security/functionality records available?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
15.	Are policies established restricting users from making certain configuration changes?	Users are authorized to make only minor adjustments to systems, and only those adjustments necessary to accomplish assigned tasks.		
16.	Are policies established granting users authorization to add peripherals and software?	Restrictions are in place showing what peripherals and software users can add to PDA systems.		
17.	Do users receive training on PDA usage and security requirements?	Verification that the user has been trained in basic functionality and data security requirements.		
18.	Are procedures established for allowing personnel to connect internally (from their own office space) to USDA ADP resources using PDA systems?	Written authorization allowing the user to access resources.		
19.	Are PDA connections authorized through private domain services (Individual VPN services)?	Access to resources is authorized through private domain services following strict guidelines to accomplish organizational tasks.		
20.	Are data synchronization procedures in place and properly configured?	Systems are properly configured for data synchronization.		
21.	Are user profiles properly configured for docked/un-docked systems?	User profiles are configured according to manufacturers and local policy specifications.		
22.	Are systems with wireless modems pre-configured using the proper configurations?	Software and hardware are both pre-configured		
23.	Are there established access hours for remote PDA users?	RAS servers are configured to allow access during only authorized times.		
24.	Are system/application security features pre-configured for the user by an experienced technician?	Software and hardware are both pre-configured		
25.	Are users restricted from disabling encryption settings on a per-application basis?	Users should not be allowed to change encryption settings.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
26.	Do systems provide per record decryption capabilities?	Systems should decrypt only those records being used. If the system were stolen or lost, access would be limited to only the most recent working record.		
27.	Are systems properly disposed of per local policy?	PDA's found to be inoperative per functionality and performance standards are properly sanitized and disposed of per local policy.		
28.	Are records available showing prior system security/ functionality checks?	Systems technicians have updated reports of systems maintenance/ security/functionality checks.		
29.	Are users instructed on procedures to take in cases of lost or stolen PDA system?	Users understand the course of action for reporting lost or stolen systems per local policy.		
30.	Do local policies require personnel wishing to connect to USDA ADP resources with privately owned PDA systems to receive prior approval?	Personnel requesting to use privately owned PDA systems to connect to USDA ADP resources require the same prior approval as those personnel using organizational issued PDA's.		
31.	Are privately owned PDA systems required to meet the same functionality/ performance standards as organizational issued PDA's?	Policy addressing requirements for using a personally owned PDA with minimum acceptable standards.		
32.	Are privately owned PDA systems checked by IT security personnel prior to being authorized connection into USDA ADP resources?	Privately owned PDA systems are checked for serviceability, unauthorized software, virus protection software, password specifications, and to ensure they meet required configuration settings to connect through resources or external VPN.		
33.	Are owners of privately owned PDA systems informed that their systems are subject to	Personnel using privately owned PDA's should be under the		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	periodic security checks?	same guidelines as organizational issued PDA's with regards to periodic security checks to ensure that conformance standards are being met.		
34.	Are the same security requirements established for organizational issued PDA's required for privately owned systems?	Users of privately owned PDA systems should have the same security requirements to connect to local resources. This will include the use of authentication procedures to connect, safeguarding of data, only authorized software systems, virus scanning software, etc.		

Comments:
Action Plan:

ATTACHMENT 1

Legal Notice Text string:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT…

Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER